CHAPTER 16
Information and Communications Technology Policy

A. Policy Statement

The City shall maintain its information and communications technology environment to enable efficient, secure, legally compliant, and effective work by staff. The function of the Information Technology Department (IT) is to fulfill these technology, communications, and collaboration needs in a well-planned manner.

B. Key Definitions

1. ***Access Control***. Limits placed on the ability to interact with networks, hardware, and/or software. Limits can be physical or logical in nature, affecting access to computing hardware, resources on data networks, entry into and use of business software, and ability to work with data.

2. ***Backup***. A copy of original content that is transferred to a separate location(s) and/or medium(s) to safeguard the content for later restoring information in the event of unwanted deletion, alteration, or disaster.

3. ***De Minimus Use***. Personal employee use of City IT resources that is nominal, irregular, and within ethics standards.

4. ***Information Systems***. Computer hardware, software, storage, networking, procedures and processes used in collecting, processing, storing, sharing, or distributing information.

5. ***Information Security Officer (ISO)***. City employee(s) designated by the Chief Information Officer to serve as the point-of-control for technology-related security issues. The individuals are designated in IT employee listings.

6. ***Malware***. Any code, script, or other software that disrupts proper operation of systems, provides unauthorized access to network and/or systems, gathers/shares information without knowing consent, or otherwise causes undesired and compromising activity.

7. ***Mobile Devices***. Portable communications and computing devices, such as cellular-based smartphones, tablet computers, and portable personal network cards/peripherals.

8. ***Password***. A sequenced combination of characters and numbers used to confirm that a user requesting access to a network or system is permitted to do so. Typically, a unique User Access Account is paired with a password to manage access. The password, known only to the user who generated it, is entered to verify identity. A password is deemed "strong" if requirements for length, character use, and pattern significantly impede malicious and/or unintended access.

9. ***Private and Sensitive Data***. Information defined by law, policy, or regulation as warranting controls over access, storage, release, modification, destruction, loss, and/or misuse.

10. ***Technology Assets and Resources***. The City's computers, servers, mobile devices, printers, computing peripherals, software and licenses, data communications network, technology vendor contracts, and services agreements.

11. ***User Access Account***. An electronic identity used to access to specific resources. Paired with a password and/or additional means of authentication, User Access Accounts allow secure use of information assets, resources, and tools.

C. Information and Communications Technology Usage

1. Accountability. All employees are responsible for all activity occurring under their User Access Accounts. For information security purposes, employees **shall not** permit or make it convenient for individuals to use accounts not assigned to that person.

2. Privacy. No person using City technology and communications resources has any right or claim to privacy. Conduct on City resources, at City facilities, and/or during work time is subject to monitoring and recording as approved by the City Manager and/or designee(s).

3. Appropriate Use. City employees shall use City technology assets and resources in a professional, legal, and ethical manner. Misuse of technology assets and resources may result in discipline up to and including termination. The following are expressly prohibited:

    a. Originating or relaying materials that discriminate or cause discrimination as defined under local, state, and Federal laws.

    b. Originating or relaying intimidating, hostile, and/or threatening communications.

c. Altering messages to attribute and relay incorrect information~~;~~.

d. Violating copyrights, trademarks, or licenses.

e. Knowingly introducing malware and security risks into the City technology and communications environment.

f. Accessing the secure files and/or the communications of others without prior approval by the City Manager or designee.

g. Using City technology and communications resources to benefit personally, apart from employment terms.

h. Using City technology and communications resources of assigned work hours without current supervisor permission.

i. Any political activity defined as inappropriate under local, state, and Federal laws, and not approved as part of the City's approved legislative efforts.

4. Personal Use. The technology and communications resources of the City are for business use. De minimus personal use is permitted if extenuating circumstances exist and provided the employee does not violate Federal or state laws. It is the responsibility of the employee to ensure the limits on personal usage of public assets are understood prior to making such use.

5. Informal Communications. Instant messaging, voice mail, and text messages are informal tools for coordination purposes. Communications on these tools may fall under Arizona Public Records laws and corresponding retention schedules.

6. Recording. City of Avondale employees may not record images or sound of City work, programs, services, projects, employees or activities while in the course and scope of their employment unless it is for City business purposes and is either: (1) specifically authorized in writing by their supervisor or manager or (2) pursuant to department policy. Such recordings may fall under the Arizona Public Records laws and corresponding retention schedules.

   Absent preauthorization, when urgent circumstances reasonably prevent the employee from first seeking the prior written approval from their supervisor or manager for the specific use in question, employees may record the images and sound and obtain approval after the fact.

7. Preventative Monitoring. IT shall maintain solutions to prevent malware and to filter materials of a discriminatory, prohibited, and/or illegal nature.

If activities of these types are detected, employee conduct will be addressed by the employee's managers and the Human Resources Department.

8. Telecommuting. Support for employees to work from home can benefit City services and operations by improving staffing flexibility in desired situations. If granted by the City to sustain operations, IT shall maintain the ability for required employees to remotely and securely access the City network to perform essential job functions. Specialized costs in addition to core network services are to be addressed by the requesting department and IT. Any employee approved for and who accepts a telecommuting assignment is responsible for ensuring the security of City assets at all times.

9. Research and Development. Exceptions to Chapter 16 may be allowed to support testing of new technologies. The purposes of these initiatives are to pilot viability of new services, improve existing services, and/or reduce costs. In all instances, testing must be approved by the City's Chief Information Officer, not interfere with City operations, and ensure private and sensitive data is not placed at risk.

D. Information and Systems Security

1. Intent. IT shall ensure the City's technology and communications environment is secure, reliable, and usable.

   a. Information Security Officer. The City shall name an Information Security Officer (ISO) and at least one alternate to coordinate information security efforts, address security incidences as they occur, and complete investigations approved by the City Manager and Chief Information Officer, or their designee(s).

   b. Access. Permissions shall be based on an assessment of the City's potential exposure to unauthorized access, theft, destruction, alteration, or misuse of information resources.

      i. Security and controls shall be applied in a least-permissive manner. Employees, interns, volunteers, and contractors shall be granted and exercise only those rights needed to perform their assigned duties and to perform required administrative tasks.

      ii. Critical technology assets and resources – e.g., servers, security gateways, network equipment, system consoles – shall be physically secured in protected areas with access logging. Security designs must be approved through IT.

iii. Employee technology and security training is required at least annually and shall be tracked by the Human Resources Department.

iv. Only personnel authorized by IT shall have access to the City data center, network closets, server rooms, control centers, or network operation centers.

v. The Human Resources Department, Facilities Division, and IT shall coordinate a program for badges and physical access controls for the City.

c. Access Forms. All employees, volunteers, interns, contractors, and other users of the City IT resources shall be required to sign an acknowledgment of the City's Information and Communications Technology Policy prior to starting work for the City.

i. Signed employee, volunteer, and intern forms are to be maintained by the Human Resources Department.

ii. Signed contractor forms are to be maintained by IT. Individual access may not exceed six months, after which access must automatically terminate, unless departments review and reauthorize access.

iii. IT shall review associated forms at least annually and shall maintain the forms on the City Intranet for easy access and use.

d. Notification. Hiring managers and supervisors must submit signed forms to IT at least three work days prior to the arrival, reassignment, and separation of all employees, interns, and volunteers.

e. Secure Computing. All computing devices connecting to City technology networks and assets must have appropriate countermeasures installed and active as deemed appropriate by IT under applicable agreements or standards. Countermeasures must include the following:

i. Anti-malware, anti-virus, email scanning, and firewall software/hardware.

ii. Secure password usage.

iii. Setting to purge or lock device if an incorrect password is used excessively.

iv. Active permissions allowing IT to remotely wipe City information.

v. Pre-boot encrypted hard-drives for City-owned computers.

f. External Security Requirements. IT shall be responsible for coordinating all external security requirements placed on the City, including audits and any mandates from state and/or Federal agencies.

2. Position Coordination. The Human Resources Department shall consult with IT when filling positions that are technology-focused. IT shall ensure that consistent position descriptions exist for City technical staff, individuals with appropriate technical qualifications are hired for City IT positions, and security needs for specialized positions required by City departments are properly addressed.

3. Incident Response. IT shall be the central authority for computer and data security.

a. Definition. An incident is defined as any event wherein the security of City data, hardware, software, and/or network is potentially compromised. This includes suspected malware infection, loss/theft of a computer(s), loss/theft of data media, discovery of inappropriate sharing of private and confidential data, etc.

b. Employee Responsibility. City employees and departments are responsible for notifying the IT Help Desk and/or Information Security Officer of any malware infections, hardware loss, or data loss upon discovery.

c. Coordination. IT shall notify the City Manager, City Clerk, and City Attorney of any security incident that rises to the level of security breach, as defined under Arizona law. The City Attorney and IT will coordinate to fulfill legal requirements as needed. In such an event, the responsible department shall be first to cover expenses to address the breach.

4. Technology Acquisitions. IT shall serve as the central authority for acquisition, asset management, and licensing compliance of City technology assets. City departments shall work with IT to minimize

redundant technology purchases in favor of enterprise-wide, secure, and economical approaches. The Finance and Budget Department, City Attorney, and IT shall jointly ensure the City's interests are protected in technology-related contracts.

a. Approval. All technology hardware, software, and services for use by the City must be approved through IT prior to procurement and purchase.

b. Procurement. IT shall have a voting member on all procurement selection committees for software, technology hardware, and/or technology services. The role of IT in procurements is to ensure successful integration and execution of technology-related projects, systems, and services. All technology -related purchases must comply with the requirements of the Avondale Procurement Code (Municipal Code, Chapter 25) and Procurement Administrative Policy.

c. IT Asset Management. IT shall be responsible for the following IT Asset Management functions:

    i. Accepting delivery of technology assets.

    ii. Maintaining accurate asset inventories and tracking.

    iii. Complying with all appropriate licensing requirements.

    iv. Disposing of hardware in an environmentally-responsible manner.

    v. Restricting software, hardware, and services that unnecessarily compromise the security and/or reliability of the City's information technology environment.

    vi. With the Finance and Budget Department, maintaining cost allocation and capital plans for the City's software licensing, hardware replacements, and central services funds.

d. External IT Services. For all vendor-provided products and/or services, City departments are responsible for working with IT to ensure:

    i. Security of City information and data.

    ii. Appropriate vendor staff expertise.

iii. Required performance.

iv. Preservation of data by the City upon conclusion of services.

v. Contractual allowances for migration to alternative, future services.

vi. Adequate long-term funding to maintain services.

5. Audits. IT will ensure the City's compliance for secure computing and licensing.

a. IT shall conduct audits of physical, network, system, data, application, and operational information systems security at least once every two years. Results will be shared with the City Manager and department directors for corrective action.

b. IT shall periodically review licensing for software and services to verify the City meets required obligations and limits under its service agreements and contracts.

6. Review of Use. Requests to examine a specific employee's use of City technology and communications resources must be approved by the City Manager~~,~~ and the Human Resources Director, or their respective designee(s).

E. IT Asset Allocation

1. Computers.

a. Primary Use Computers. Centrally allocated computers shall be those assigned to employees for the primary performance of their duties. Computers are to be budgeted and assigned on a one computer per FTE basis.

b. Special Use Computers. Special Use hardware are those devices deemed necessary by departments for specific, non-convenience uses – e.g., grant-funded programs, Council Chambers, library patron use, unique public safety and public works field applications, et al. Special Use computers must be approved by the responsible department director and IT prior to purchase and paid for from respective department operating funds, unless otherwise arranged through the Finance and Budget Department.

c. Standard Specifications. IT is charged with responsibility for setting standard specifications for computers, and including assignment of desktop/laptop/virtual units.

d. Lifecycle. Computers are to be managed, inventoried, and maintained through IT . Computers shall be replaced on an equipment lifecycle defined by IT. The lifecycle shall balance costs and the usable life of equipment.

e. Inventory Recovery. Computers replaced shall be reclaimed by IT for secure disposal, ensuring equipment has not been lost/stolen, and for removing assignments of licensed software. Departments may temporarily retain replaced computers for short periods in special circumstances, as approved by IT.

f. Technology Replacement Fund. Replacement costs for Primary Use computers shall be budgeted for and charged to departments as part of the City's annual capital plan. Cost allocations shall be set in the City's budget by the Finance and Budget Department and IT, with City Council and City Manager approval.

2. Servers, Communications Hardware, and Reprographic Equipment.

a. Efficient Deployment. Servers, telecommunication equipment, and multi-function printers/copiers/scanners shall be managed, inventoried, and maintained through IT. All departments are responsible for minimizing costs while meeting functional needs in specific areas of the City organization.

b. Special Uses. Departments may request and pay for specialized equipment and service in specific areas through IT. Special Use equipment must be approved by IT prior to purchase and paid for from respective department operating funds, unless otherwise arranged through the Finance and Budget Department.

c. Lifecycle. Servers, telecommunication equipment, and multi-function printers/ copiers/scanners shall be replaced on an equipment lifecycle defined by IT–in administrative procedures. The lifecycle shall balance costs and the usable life of equipment.

d. Technology Replacement Fund. Replacement costs for servers, communications hardware, and reprographic equipment shall be budgeted for and charged to departments as part of the City's annual capital plan. Cost allocations shall be set in the City's budget by the

Finance and Budget Department and IT, with City Council and City Manager approval.

3. Mobile Communications and Computing.

a. Provision. Mobile devices should not be purchased by the City except for special needs. Technology stipends should be used as the standard solution to address needs for key department personnel to be reachable and/or have extra mobility for work purposes. Departments are responsible for minimizing costs while meeting these functional needs.

b. Approval Process. Requests for stipends and reimbursements should be submitted by employees via their department director to IT, the Human Resources Department, and the City Manager for approval. Hourly employees may not access City resources outside of working hours unless otherwise approved by their respective department. Mobile communications and computing devices should be paid for from respective department operating funds, unless otherwise arranged through the Finance and Budget Department.

F. Records Administration

1. Intent. IT shall maintain City information and data to support operating needs, including disaster recovery, business resumption, and data loss prevention. Standards shall be set between the City Clerk and IT to meet requirements and standards set by ARIZ. REV. STAT.§ 39-101, as well as departmental needs.

2. Archiving and Recovery. IT shall configure systems to save central data and information to recover from corruption and loss. Recovery will include full, incremental, and differential backups to allow the City to restore to past days, weeks, months, and years as required by records retention schedules published by the Arizona State Library, Archives and Public Records and administered by the City Clerk. IT is charged with conducting central backups, testing backups for the ability to successfully restore systems and information, ensuring the ability to resume business in the event of a disaster, and maintaining the ability to retrieve information from required legacy files and formats. City employees are charged with ensuring their work products and information are saved to central IT resources to be backed up and archived.

a. Email. Electronic messages will be saved per the current records retention schedules published by the Arizona State Library,

Archives and Public Records and coordinated by the City Clerk. Storage options will be provided for longer-term storage as determined necessary by the City Clerk and departments.

b. Files. Electronic files will be saved per the records retention schedules published by the Arizona State Library, Archives and Public Records and coordinated by the City Clerk. Archived files will consist of most recent backup copies and year-end copies.

c. Databases. Databases will be saved per the current records retention schedules published by the Arizona State Library, Archives and Public Records and coordinated by the City Clerk. Archived databases will consist of most recent backup copies and a defined schedule of periodic copies.

3. Records Hold. The City Attorney and IT shall provide processes and tools for saving files related to known legal actions. The City Clerk, City Attorney, and City departments will train to appropriately manage departmental files and information to comply with legal requirements.

G. IT Protocols and Guidelines

1. IT Administrative Policies and rules shall be reviewed and updated at least annually to ensure they continue to meet the requirements of the City and its departments.

2. IT shall maintain and publish operating guidelines to employees via the City Intranet. Standard guidelines include those of the following:

a. Standard specifications for computers used by employees by utilization type – e.g., administrative computers, GIS/developer/engineer workstations, and semi-rugged and fully-rugged computers

b. Support for Mobile Communications Devices

i. Advanced support for smartphones and tablet computers.

ii. Supported service for access to City email, schedules, and contacts.

iii. Supported online storage services for saving work for backup and public records searches.

iv. Supported note-taking and mark-up applications.

v. Supported wireless access methods.

c. Security Standards

i. Security Signature Forms .

ii. Password Complexity and Expiration.

iii. Incident Response and Monitoring Processes.

iv. Access Audits.

d. Technology Reimbursements and Stipends

i. The City Manager shall set technology and telecommunications stipend/reimbursement standards for the City to address eligibility, stipend and reimbursement rates, approval process, and authorization forms to be used.